BACKGROUNDER

Published by the Truman National Security Project

Surveillance Law for the 21st Century:
RESTORE Protects Our Security AND Our Liberties

John Neffinger and Jessica Tacka, Truman National Security Project

16 October 2007

This week Congress considers a well-crafted and desperately needed bill to restore government accountability and American liberties while also allowing for the robust and vigorous surveillance of modern terrorist networks. The RESTORE Act, or H.R. 3773, curtails the unconstitutional excesses of the Protect America Act, or PAA, while addressing the security shortcomings of the original FISA bill passed in an age before cellphones or the internet.

KEY POINTS

• **RESTORE Empowers Our Intelligence Agencies to Go After Terrorists, Right Up to the Constitutional Limit.** The only thing RESTORE does not allow is spying on Americans without good reason, which is prohibited by the 4th Amendment - all other intelligence gathering methods are allowed. Congress cannot grant the President any broader intelligence gathering authority than it does under RESTORE: anything more would require a constitutional amendment.

• **The Administration Can Collect All Needed Intelligence, But Must Report What They Do.** Under RESTORE, the Administration has broad latitude to conduct surveillance operations. All RESTORE requires is that the FISA court, the Department of Justice and Congress are kept in the loop. This will not only prevent violations of Americans' rights, it will also help Congress make sure the bill works well, so Congress can take appropriate steps when RESTORE comes up for reauthorization in 2009.

I. Background to the Foreign Intelligence Surveillance Act (FISA)

In the wake of Watergate and the revelation that the Nixon administration had been spying on Americans in violation of the Constitution, Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA), which established a special court and specific procedures to govern the gathering of foreign intelligence-physical or electronic-inside the United States. Under the original FISA, intelligence gathering that occurred *entirely outside* the United States was largely unregulated.

As opposed to law enforcement surveillance authorizations, authorities do not need to believe a crime has been committed to have probable cause for FISA surveillance. Approval is determined by the Foreign Intelligence Surveillance Court (FISC), a specialized court staffed by eleven federal judges, so long as three major conditions are met:

1. There must be "probable cause" that the target is a foreign power or an agent of a foreign power. For a U.S. citizen to be directly targeted under FISA, they must also be suspected of committing a crime.

2. A "significant purpose" of the surveillance must be the collection of foreign intelligence.

3. Procedures must be followed to ensure that information collected about U.S. persons (a citizen, permanent resident, or corporation) is minimized.

FISA already has mechanisms to ensure that congressional oversight and judicial review do not impede the ability of the intelligence community to move swiftly in response to threats:

- In emergency situations, surveillance may proceed for up to 72 hours while a warrant application is pending before the FISC.

- The Attorney General and Director of National Intelligence (DNI) are also permitted to authorize electronic surveillance for up to one year in the U.S. *without a court order* so long as they certify under seal to the FISC that the conditions listed above are met, and that "there is no substantial likelihood that the surveillance will acquire the contents of any communication" to a U.S. person, classified as a U.S. citizen or permanent resident.

These provisions give the President the flexibility, secrecy, and discretion necessary to ensure national security, while at the same time permitting the judicial review and Congressional oversight that preserve civil liberties. From 1978 to 2006, the FISC granted nearly 19,000 warrants and rejected only five. That is fewer than 1 rejected application for every 3,000 submitted.

Triggered by the NSA illegal wiretapping scandal, and the understanding that U.S. intelligence agencies require a modernized surveillance authorization process to keep up with technological advancements, Congress passed a stopgap measure called the Protect America Act (PAA). This act created a new framework for surveilling targets that were believed to be overseas without being restricted by an outdated FISA. It was meant to enable U.S. intelligence gathering for 6 months while Congress considered how to revise and modernize FISA to allow robust surveillance to maintain American security while also protecting our constitutional liberties.

How Surveillance Situations Would be Treated Under FISA, PAA and RESTORE

Situation	FISA	PAA	RESTORE
A U.S. Soldier overseas emails home.	Individual warrants required (to surveil any U.S. person anywhere).	Soldier and family are subject to surveillance on both ends with no warrant.	Individual warrants are required to surveil any U.S. persons, even overseas.
Suspected terrorists abroad spoof IP address to indicate a U.S. location.	FISA warrant is required if the signal appears to go through the U.S.	No warrant is required if there is reasonable belief these are non-US Persons outside the U.S.	No warrant required if there is reasonable belief these are non-US Persons outside the U.S.
U.S. student studying abroad in Jordan writes to family back in the U.S. DNI looking for terrorist cells in Jordan.	Cannot surveil or physically search family in the U.S. without individual warrants and evidence of criminal acts.	Student and family are subject to surveillance under umbrella warrants. Family may be at risk for physical search and seizure without a warrant.	Family will not be at risk for physical search and seizure of their property, nor will student be included in an umbrella warrant seeking FII from agents of Jordan.
DNI wants to collect all communications from Hotmail accounts looking for evidence of terrorist plots.	The DNI could apply to the FISA Court for authorization to collect information on individual suspects. DNI has no rights to information about U.S. person NOT involved in criminal acts.	The government could collect all of Hotmail's records of communication from anyone reasonably believed to originate outside the U.S. This information could remain on file indefinitely, even if a U.S. citizen were involved or targeted.	Original FISA requirements whenever a U.S. citizen was involved, at home or overseas. Umbrella warrants could be obtained for searches targeted at communications from non-U.S. person overseas.

II. Why Did FISA Need to Be Changed… And What Has the Protect America Act Done?

FISA needed to be changed to address two major developments since the Act was first passed three decades ago. The Protect America Act (PAA), a six-month sunset law signed into effect in August 2007, fixed some of these issues, yet also created a host of new concerns that need to be addressed in a more permanent piece of legislation.

Two Problems PAA Fixed:

1) PAA Removed the Need to Know The Exact Identity of The Person Under Surveillance:

To authorize surveillance, a subject had to be a foreign agent, and his or her location had to be known. But the primary goal of intelligence gathering against suspected terrorists is to determine whether a given target is in fact a terrorist, whether or not they operate on behalf of a state, and where that person is located if they are dangerous. Under unreformed FISA, the information required for authorization is exactly the same information the surveillance would seek to discover.

The Need for Oversight

During his Spring 2005 UN Ambassador confirmation hearings, John Bolton admitted that on a number of occasions when he was at the State Department he had received reports of NSA intercepts between an individual in a foreign country and an individual in the U.S. In keeping with minimization guidelines, the identity of the U.S. speaker had been redacted and replaced with the generic "U.S. person." But Bolton wanted names. The NSA turned them over to him at his request to better understand the context of the conversation, no questions asked. Following this revelation, Newsweek reported that between January 2004 and May 2005, the agency had supplied the names of some 10,000 American citizens in this informal manner to various interested parties in Washington.

PAA Solution: Instead of being required to know detailed information about the target and his or her location to obtain authorization for surveillance, the PAA allows for sweeping surveillance of anyone, not specifically a foreign power or agent of a foreign power, reasonably believed to be outside the U.S. This is called an "umbrella warrant" and can include one or many subjects.

2) PAA Changed the Location Requirements Under FISA: The rise of the Internet has made it both more difficult and less compelling to make the warrant requirement turn solely on the location of surveillance activities.

- Because email can be sent from anywhere on Earth, it is far more difficult to know whether a particular party sending or receiving a communication is in the United States or not, and therefore whether FISA applies.

- Because the Internet may route packets of information through servers housed in the United States, FISA might have applied to electronic communications *even when all parties involved are located abroad*. Without change, any communication that appeared to route through the U.S. would be subject to FISA scrutiny, despite the technological advances that can be used to mask an individual's location.

- For instance, suppose a suspected foreign agent in Pakistan communicates using a "spoofed" or falsified Internet protocol (IP) address that alleges a New York location. Under unreformed FISA, terrorists could use this false location to receive the same procedural review as anyone actually in the U.S.

PAA Solution: The PAA exempts electronic surveillance "directed at a person reasonably believed to be located outside of the United States" from the requirements of FISA. Thus, if the government is monitoring someone outside the United States from a switch or router inside the United States, it can listen in on the person's calls and read their e-mails without obtaining a FISA warrant first. Before this, the actual surveillance, even of a non-citizen suspected to be outside the U.S., would have to be conducted abroad or subject to FISA limitations.

But the PAA Created Serious New Problems:

1) PAA Can Be Used Against U.S. Citizens:

The PAA exempts electronic surveillance "directed at a person reasonably believed to be located outside of the United States" from the requirements of FISA, but the statue does not define "directed at." There is also no requirement that the person at whom the surveillance is "directed" be an agent of a foreign power or in any way connected to terrorism. "Directed at" also implies unintended casualties that may include the communications of U.S. citizens, even those inside the U.S.

- Thus, if interpreted literally, a warrant is no longer required for *any* surveillance (physical or electronic) involving *anyone* in the United States for *any* reason (or no reason) as long as it is primarily "directed at" some-

one reasonably believed to be overseas.

- Although the Attorney General or DNI still has to certify that a "significant purpose" of this new, non-FISA-compliant surveillance "is to obtain foreign intelligence information," the requirement does not exclude the possibility that another purpose could also be to obtain information *not* related to foreign intelligence.

2) PAA Almost Entirely Eliminates Meaningful Judicial Review:

- If electronic surveillance of a person believed to be outside the U.S. is conducted by the government alone, it is completely insulated from any oversight or review whatsoever.

- There is *no judicial review* of umbrella warrants against overseas targets unless a communications company refuses to turn over information to the government. At that point, the review of information is extremely limited.

- Only the *procedures* used to make that determination can be reviewed, and only once annually. Moreover, the FISC is only authorized to reject procedures that are "clearly erroneous;" this is *extremely* deferential review that may have no teeth whatsoever.

- Finally, the PAA grants immunity to service providers who assist the government, giving them no reason to challenge the legal merits of a request for information. This has ramifications for the retroactive immunity of those service providers who cooperated with the NSA. Any retroactive immunity proposed or agreed to in future legislation sets a precedent for "shoot first, ask questions later" violations of civil liberties.

- The PAA enables the government to enlist the assistance of communications service providers, like phone and cable companies, for up to a year, without a warrant, so long as there are both 1) "reasonable procedures" in place to ensure that the target of a surveillance is reasonably believed to be outside the United States; and 2) procedures to ensure that information collected about U.S. citizens is otherwise minimized. Neither of these items is reviewed by the FISC.

3) PAA Deceptively Extends to February 2009, Not just 6 Months

- Not only does the PAA enable overbroad powers to the Executive Branch that may infringe on the civil liberties of U.S. persons, but its 6-month sunset clause is extremely deceptive. Each authorization is valid for one year, extending the PAA to February 2009 and encouraging generous authorization of warrantless surveillances in an effort to "beat the sunset."

III. RESTORE Fixes FISA's Security Loopholes…

"Foreign to Foreign" Communications Need no Warrant. RESTORE clarifies that the government does not need to get a warrant from the FISA court to intercept communications between foreign persons, even if they pass electronically through the United States.

"Umbrella" Warrants Are Allowed. RESTORE also provides a procedure for the FISA court to issue an "umbrella" authorization to conduct surveillance targeting foreign persons for up to one year, with the caveats that its targets must be reasonably believed to be non-U.S. persons located outside the United States, and a significant purpose of the surveillance must be to obtain foreign intelligence related to national security (i.e. not soldiers writing home). Note that this kind of umbrella warrant might still authorize the "incidental" surveillance of innocent U.S. persons

Better Enables Emergency Surveillance: Some of the changes to FISA introduced by PAA were a response to accusations that FISA endangered American lives by restricting emergency access to surveillance authorization. RESTORE more than *doubles* the time period for emergency surveillance, allowing up to 7 days of surveillance in the heat of a situation before an application must be filed, and 45 days of surveillance while the application is pending.

… And Protects Civil Liberties Lost Under the PAA

Balancing civil liberties with security in an age of changing communication is difficult. RESTORE is not perfect, but it includes a host of provisions to reduce the likelihood that the government will not misuse its surveillance powers in violation of the Constitution. RESTORE:

Prohibits Physical Searches of U.S. persons: PAA was drafted broadly enough that it could have been construed to permit physical searches in some cases that might incidentally involve U.S. persons. RESTORE clarifies that physical searches are not allowed and that only electronic surveillance is covered.

Increases FISA Court Oversight: Unlike under PAA, RESTORE requires the FISA court to issue a warrant for surveillance whenever a U.S. person is involved.

Ensures that Warrents Are Not Overly Broad: Before issuing a warrant, the FISA Court must make several specific findings designed to make sure the surveillance

is targeted and will minimize the risk of incidentally gathering information on U.S. persons without proper cause. The court must find that:

- The proposed targeting procedures are reasonably designed to target only non-U.S. persons outside the United States.

- The proposed procedures follow FISA requirements for "minimizing" the amount of irrelevant information the government acquires, retains, and disseminates.

- The proposed guidelines include provisions to seek a traditional court order to conduct surveillance of any person reasonably believed to be located in the United States.

Although U.S. persons' communications may still end up being intercepted without a warrant based on probable cause under RESTORE, these more specific requirements for a warrant reduce the potential for the government to use this power improperly for spying on Americans.

Restores Congressional Oversight: RESTORE requires the Attorney General and the Director of National Intelligence to submit compliance reports to both the Intelligence and Judiciary Committees, including reporting on incidents where procedures were not followed, incidents in which a U.S. person's information was incidentally gathered, and any time the identity of a U.S. person discovered during surveillance was shared with other government agencies.

Restores DOJ Oversight: RESTORE requires the Inspector General of the Department of Justice to conduct audits and report to both Congress and the FISA Court on the government's FISA compliance and U.S. persons caught up in government surveillance.

Includes a Sunset Clause: RESTORE also includes a "sunset" provision, terminating on December 31, 2009 unless renewed by Congress. This will allow Congress to reconsider the provisions of RESTORE in light of the information from the increased reporting requirements to determine whether the law should be revised for any reason.

Creates a Legal Basis for the Long Fight Against Terrorists: RESTORE expressly states that the FISA procedures as amended by RESTORE apply to all surveillance activities conducted by the government, and invites the President to come back to Congress to ask for additional authorizations before defying the law further.

Investigates the Administration's Potentially Unlawful Activities: Finally, RESTORE also instructs the Inspector General of the Department of Justice to investigate and report to Congress on the government's surveillance activities since 9/11 under the so-called Terrorist Surveillance Program, which did not obtain warrants from the FISA court and may well have been illegal under FISA and/or the 4th Amendment to the Constitution. This is also important to establish that such violations will not be forgotten, and will have significant consequences, even if only political.

*Please see page 6 for a comparison table between FISA, PAA and RESTORE

This Paper Can be Found at

www.trumanproject.org

Two Weeks After its Original Release Date.

By signing up as a member you can receive this paper on a regular basis upon its release.

Published by:

Truman National Security Project

1 Massachusetts Ave NW, Suite 333
Washington, DC 20001
Telephone: 202-216-9723
Fax: 202-682-1818
info@trumanproject.org

Domestic Surveillance Law: Past (FISA), Present (PAA) and Future (RESTORE) Provisions Compared

	FISA Foreign Intelligence Surveillance Act (1978)	**PAA** Protect America Act (2007)	**RESTORE** Responsible Electronic Surveillance That is Overseen, Reviewed, and Ef-fective (introduced October 2007)
Overview	Established FISA court review for surveillance inside the U.S., set out when warrants are needed.	Enabled the use of "umbrella" warrants, directed at anyone "reasonably believed" to be overseas, curtailed FISA court oversight.	Restores 4th Amendment protections to U.S. citizens, and permanent residents, and restores oversight by FISA court, DOJ, Congress.
FISA warrant needed for foreign communications routed via US?	Yes. FISA warrant needed for any "domestic" surveillance, even of foreign persons overseas	No. As long as surveillance targets reasonably believed to be non-US persons overseas, US routing immaterial.	No. As long as surveillance targets reasonably believed to be non-US persons overseas, US routing immaterial.
"Umbrella" warrants allowed?	No. Warrants must target specific individuals based on specific suspicions.	Yes. Broader surveillance allowed to establish identities and suspicions.	Yes. Broader surveillance allowed with FISA warrant if reasonably targeted at non-US persons overseas.
4th Amendment protection for U.S. citizens, permanent residents and corporations	Strict: - U.S. persons cannot be targeted unless there is a suspicion of criminal activity. - Individual warrants are required for each U.S. person surveilled.	Lacking: - Opens U.S. citizens at home and abroad to warrantless surveillance. - Opens door to warrantless domestic surveillance plus PHYSICAL search and seizure of property.	Reasonable: - Clarifies that umbrella warrants may NOT target U.S. Persons; may use info on US persons gleaned while targeting others. - Reinstates 4th Amendment protections from warrantless physical or electronic domestic searches.
FISA court review triggered by…	Any surveillance undertaken inside the U.S. When both parties are overseas, FISA does not apply.	Any surveillance of people inside the U.S. A telecom service provider's refusal to comply with DNI or AG umbrella warrant.	Any surveillance inside the U.S. and/or involving a U.S. person.
FISA court review process	When warrants are required, the FISA court must approve them individually.	FISA Court is entitled to a semi-annual review of procedures. Deferential procedural review of umbrella warrant contested by telecom service provider.	Reinstates FISA court review of all warrants except in the case of an emergency. Requires frequent reporting to the FISA court and Congress.
Authorizations available with or without subsequent FISA court review	In an emergency, surveillance may proceed for 72 hours before warrant approved. AG or DNI may approve warrantless search for 1 year after certifying to the FISA court negligible likelihood of intercepting U.S persons' communication.	Any electronic surveillance of a person believed to be outside the U.S. (Less FISA court review required.)	In an emergency, AG or DNI may authorize surveillance prior to receiving a FISA warrant. They then must apply for a warrant within 7 days.
Congressional/ DOJ Oversight	Standard Congressional oversight.	Standard Congressional oversight (with only limited information available via the FISA court because of its limited role).	DNI and AG report to Congress, detailing violations and sharing information on U.S. person's whose communications were incidentally acquired. DOJ Inspector General to conduct periodic audits, report to Congress and FISA Court.
Immunity?	None.	Telecom providers are given legal immunity if they comply with AG or DNI requests; also possible retroactive immunity for any prior illegal conduct (2001-2006).	Offers possibility to compliant service providers. There is no authorization for *retroactive* immunity.